

Embedding in a perfect code

Sergey V. Avgustinovich, Denis S. Krotov

Abstract. A binary 1-error-correcting code can always be embedded in a 1-perfect code of some larger length.

For any 1-error-correcting binary code C of length m we will construct a 1-perfect binary code $P(C)$ of length $n = 2^m - 1$ such that fixing the last $n - m$ coordinates by zeroes in $P(C)$ gives C .

In particular, any complete or partial Steiner triple system (or any other system that forms a 1-code) can always be embedded in a 1-perfect code of some length (compare with [5]). Since the weight-3 words of a 1-perfect code P with $0^n \in P$ form a Steiner triple system, and the weight-4 words of an extended 1-perfect code P with $0^n \in P$ form a Steiner quadruple system, we have, as corollaries, the following well-known facts: a partial Steiner triple (quadruple) system can always be embedded in a Steiner triple (quadruple) system [6] ([3]) (these results, as well as many other embedding theorems for Steiner systems, can be found in [4, 1]).

Notation:

- F^m denotes the set of binary m -tuples, or binary m -words.
- $\dot{F}^m := F^m \setminus \{0^m\}$, where 0^m is the all-zeroes m -word.
- F^m is considered as a vector space over $GF(2)$ with calculations modulo 2.
- $\Pi = \{\pi^{(1)}, \dots, \pi^{(m)}\} = \{(10..0), \dots, (0..01)\}$ is the natural basis in F^m .
- $n := 2^m - 1$.
- The elements of F^m will be denoted by Greek letters.
- The elements of F^n will be denoted by overlined letters, their coordinates being indexed by the elements of \dot{F}^m , e.g., $\bar{w} = \{w_\iota\}_{\iota \in \dot{F}^m}$; we assume that the first m coordinates have the indexes $\pi^{(1)}, \dots, \pi^{(m)}$, and the order of the other $n - m$ indexes does not matter (but fixed).
- $\{\bar{e}^{(\iota)}\}_{\iota \in \dot{F}^m}$ is the natural basis in F^n ; note that $\bar{e}^{(\pi^{(\iota)})} = (\pi^{(\iota)}, 0^{n-m})$.
- For any $\alpha = (\alpha_1, \dots, \alpha_m) \in F^m$ denote

$$\bar{\alpha} := (\alpha, 0^{n-m});$$

it also holds $\bar{\alpha} = \sum_{i=1}^m \alpha_i \bar{e}^{(\pi^{(i)})}$.

- $d(\cdot, \cdot)$ denotes the Hamming *distance* between two words in F^m or F^n (the number of positions in which the words differ).

The full version of this manuscript is accepted for publication in the Journal of Combinatorial Designs ©2008 Wiley Periodicals, Inc., A Wiley Company

The results of the paper were presented at the Workshop “Coding Theory Days in St. Petersburg”, Oct. 2008, St. Petersburg, Russia.

The authors are with the Sobolev Institute of Mathematics, Novosibirsk, Russia. E-mail: {avgust,krotov}@math.nsc.ru

- $\langle \dots \rangle$ denotes the linear span of the vectors or sets of vectors between the angle brackets.
- The *neighborhood* $\Omega(M)$ of a set $M \subset F^n$ is the set of vectors at distance at most 1 from M .
- A set $C \subset F^m$ is called a 1-*code* if the neighborhoods of the codewords are disjoint.
- A 1-code $P \subset F^n$ is called a 1-*perfect code* if $\Omega(P) = F^n$; in this case, $|P| = 2^n/(n+1)$.
- The *Hamming code* H defined as

$$H := \{\bar{c} \in \{0, 1\}^n \mid \sum_{\alpha \in \dot{F}^m} c_\alpha \alpha = 0^m\} \quad (1)$$

is a linear 1-perfect code.

- For any ι from \dot{F}^m the *linear ι -component* of H is defined as

$$R_\iota := \{\bar{c} \in H \mid c_\alpha = c_{\alpha+\iota} \text{ for all } \alpha \in F^m \setminus \langle \iota \rangle\}$$

(note that R_ι is a linear subcode of H , for all ι). Since [7], linear components are used for constructing non-linear 1-perfect codes. For the first time, the method of synchronous switching nonintersecting linear i -components with different i , which is exploited in this paper (to follow our notations, we replace i by Greek letters), was used in [2]. Since our definition of linear components differs from others, we should prove the main property of R_ι (in essence, the following lemma coincides with [2, Corollary 3.4]):

Lemma 1. *For any \bar{z} from F^n it holds that $\Omega(R_\iota + \bar{z}) = \Omega(R_\iota + \bar{z} + \bar{e}^{(\iota)})$.*

Proof: Without loss of generality, assume $\bar{z} = 0^n$. Denote $\bar{e}^{(0^m)} := 0^n$. Then, we have

$$\Omega(R_\iota) = \bigcup_{\kappa \in F^m} (R_\iota + \bar{e}^{(\kappa)}) = \bigcup_{\kappa \in F^m} (R_\iota + \bar{e}^{(\iota)} + \bar{e}^{(\kappa+\iota)}) = \bigcup_{\lambda \in F^m} ((R_\iota + \bar{e}^{(\iota)}) + \bar{e}^{(\lambda)}) = \Omega(R_\iota + \bar{e}^{(\iota)})$$

because $\bar{e}^{(\iota)} + \bar{e}^{(\kappa)} + \bar{e}^{(\kappa+\iota)} \in R_\iota$ for all $\kappa \in F^m$. \triangle

Lemma 2. *Every element \bar{c} of $\langle R_\iota, R_\kappa \rangle$ satisfies*

$$c_\alpha + c_{\alpha+\iota} + c_{\alpha+\kappa} + c_{\alpha+\iota+\kappa} = 0 \text{ for all } \alpha \in F^m \setminus \langle \iota, \kappa \rangle \quad (2)$$

Proof: By the definition, the elements of R_ι and R_κ satisfy (2). Thus, the elements of their linear span also satisfy (2). \triangle

The following lemma is the crucial part of our reasoning.

Lemma 3. *For any $\iota, \kappa \in \dot{F}^m$ at distance at least 3 from 0^m and from each other, the ι -component $R_\iota + \bar{\iota} + \bar{e}^{(\iota)}$ and the κ -component $R_\kappa + \bar{\kappa} + \bar{e}^{(\kappa)}$ are disjoint and do not contain 0^n .*

Proof: By general algebraic reasons, it is enough to show that $\bar{w} := \bar{\iota} + \bar{e}^{(\iota)} + \bar{\kappa} + \bar{e}^{(\kappa)}$, does not belong to $\langle R_\iota, R_\kappa \rangle$. Let j be a nonzero coordinate of $\iota + \kappa$. Then $\pi^{(j)}$ is the index of a nonzero coordinate of \bar{w} ; the indexes of the other nonzero coordinates also belong to $\Pi \cup \{\iota, \kappa\}$. But, since the mutual distances between 0^m , ι , κ , and $\iota + \kappa$ are not less than 3, the indexes $\pi^{(j)} + \iota$, $\pi^{(j)} + \kappa$, $\pi^{(j)} + \iota + \kappa$ do not belong to $\Pi \cup \{\iota, \kappa\}$. So, we have $w_{\pi^{(j)}} + w_{\pi^{(j)}+\iota} + w_{\pi^{(j)}+\kappa} + w_{\pi^{(j)}+\iota+\kappa} = 1 + 0 + 0 + 0 = 1$, and, by Lemma 2, $\bar{w} \notin \langle R_\iota, R_\kappa \rangle$.

By a similar argument, neither $R_\iota + \bar{\iota} + \bar{e}^{(\iota)}$ nor $R_\kappa + \bar{\kappa} + \bar{e}^{(\kappa)}$ contains 0^m . \triangle

Theorem. Let $C \subset F^m$ be a 1-code containing 0^m ; put $\dot{C} := C \setminus \{0^m\}$. Then the set

$$P(C) := \left(H \setminus \bigcup_{\iota \in \dot{C}} (R_\iota + \bar{\iota} + \bar{e}^{(\iota)}) \right) \cup \bigcup_{\iota \in \dot{C}} (R_\iota + \bar{\iota})$$

is a 1-perfect code in F^n . Moreover,

$$C = \{\iota \in F^m \mid (\iota, 0^{n-m}) \in P(C)\}. \quad (3)$$

Proof: We note that, by (1), $\bar{\iota} + \bar{e}^{(\iota)}$ belongs to H for all ι ; so, $R_\iota + \bar{\iota} + \bar{e}^{(\iota)} \subset H$ for all ι .

By Lemma 3, the sets $R_\iota + \bar{\iota} + \bar{e}^{(\iota)}$, $\iota \in \dot{C}$, are mutually disjoint. Since they are subsets of a 1-perfect code, their neighborhoods are also mutually disjoint. Taking into account Lemma 1, we see that $P(C)$ is a 1-perfect code by the definition.

It is easy to see that

(*) *the only word in H that has the form $(\alpha, 0^{n-m})$ is the all-zeroes word.*

Furthermore, only $\bar{\iota}$ has such form in $R_\iota + \bar{\iota}$, i.e.,

(**) *if for some $\kappa \in F^m$ we have $(\kappa, 0^{n-m}) \in R_\iota + \bar{\iota}$, then $\kappa = \iota$.* Indeed, assume that $\bar{\kappa} = (\kappa, 0^{n-m}) \in R_\iota + \bar{\iota}$. Then $\bar{\kappa} + \bar{\iota} \in R_\iota \subset H$. By (*), we have $\bar{\kappa} + \bar{\iota} = 0^n$, which proves the claim (**).

From (*) and (**) we conclude that (3) is implied by the definition of $P(C)$. \triangle

References

- [1] C. J. Colbourn and A. Rosa. *Triple Systems*. Clarendon Press, Oxford, 1999.
- [2] T. Etzion and A. Vardy. Perfect binary codes: Constructions, properties and enumeration. *IEEE Trans. Inf. Theory*, 40(3):754–763, 1994. DOI: 10.1109/18.335887.
- [3] B. Ganter. Finite partial quadruple systems can be finitely embedded. *Discrete Math.*, 10(2):397–400, 1974. DOI: 10.1016/0012-365X(74)90130-7.
- [4] C. C. Linder. A survey of embedding theorems for Steiner systems. In C. C. Linder and A. Rosa, editors, *Topics on Steiner Systems*, volume 7 of *Ann. Discrete Math.*, pages 175–202. North-Holland, 1980.
- [5] P. R. J. Östergård and O. Pottonen. There exist Steiner triple systems of order 15 that do not occur in a perfect binary one-error-correcting code. *J. Comb. Des.*, 15(6):465–468, 2007. DOI: 10.1002/jcd.20122.
- [6] C. Treash. The completion of finite incomplete Steiner triple systems with applications to loop theory. *J. Comb. Theory, Ser. A*, 10(3):259–265, 1971. DOI: 10.1016/0097-3165(71)90030-6.
- [7] Yu. L. Vasil’ev. On nongroup close-packed codes. In *Problemy Kibernetiki*, volume 8, pages 337–339. 1962. In Russian, English translation in *Probleme der Kybernetik*, 8: 92–95, 1965.